Problem Set 3
CS 579: Computational Complexity

Assigned: March 13, 2014 Due on: March 31, 2014

Instructions: Please do not turn in solutions to the practice problems.

Practice Problems

Practice Problem 1. Show that $\mathbf{NP}^{\Sigma_k^p \cap \Pi_k^p} = \Sigma_k^p$ for all $k \geq 1$.

Practice Problem 2. Prove that $\mathbf{NSPACE}(s(n)) \subseteq \mathbf{ATIME}(s(n)^2)$, for proper complexity functions s such that $s(n) \geq \log n$.

Homework Problems

Problem 1. Barrington's Theorem is a surprising result that connects (non-uniform) $\mathbf{NC}_1$ with bounded width, polynomial sized branching programs. In this problem you will prove this result.

We begin by defining branching programs. A *branching program* is a directed acyclic graph in which each node is labelled by a variable x_i, one of these is designated as the *start node* and there are two special nodes labelled "accept" and "reject." All of the nodes labelled with variables have exactly two outgoing edges, one labelled "0" and the other labelled "1". An input $x = x_1x_2\dots x_n$ defines a path from the start node to the accept or reject node as follows: at every node labelled x_i, we follow the outgoing edge whose label coincides with the value of x_i in the input. If we reach the accept node, the input is accepted; if we reach the reject node, the input is rejected. Polynomial-size branching programs capture **L/poly** (logspace machines with polynomial advice) in the same way that polynomial-size circuits capture **P/poly**.

In this problem we will consider a *very* restricted subclass of polynomial-size branching programs. With the exception of the accept and reject nodes, all of the nodes will be divided into levels $\ell_1, \ell_2, \dots \ell_m$, with each level containing *at most 5 nodes*; the only permitted edges are directed from a node in level ℓ_i to a node in level ℓ_{i+1}, or a node in level ℓ_m to either the accept or reject nodes. Barrington's theorem says that width 5 branching programs exactly capture (non-uniform) $\mathbf{NC}_1$. Prove this result by solving the following parts.

1. Recall that S_5 is the group of permutations on the elements $\{1, 2, 3, 4, 5\}$. We will specify a sequence of m *instruction* triples (i_j, σ_j, τ_j), $j = 1\dots m$, where $\sigma_j, \tau_j \in S_5$ and $1 \leq i_j \leq n$. On an input $x = x_1x_2\dots x_n$ the instructions *yield* the permutation $\pi_1\pi_2\dots\pi_m$, where $\pi_j = \sigma_j$ if $x_{i_j} = 0$ and $\pi_j = \tau_j$ if $x_{i_j} = 1$. We say that the sequence of instructions π-*accepts* a set $A \subseteq \{0,1\}^n$ if every $x \in A$ yields π and every $x \notin A$ yields the identity permutation e (and $\pi \neq e$). Verify that if there is a sequence of m instructions that π-accepts A, then there is a width-5 branching program with m levels that accepts A.
2. Recall that every permutation can be written as the product of disjoint cycles. We will be concerned with elements of S_5 that are 5-cycles. Examples of these elements are $\sigma = (1\ 2\ 3\ 4\ 5)$ or its inverse $\sigma^{-1} = (1\ 5\ 4\ 3\ 2)$. Show that if π is a 5-cycle, and a sequence of m instructions π-accepts A, then for any 5-cycle $\pi' \in S_5$, there is a sequence of m instructions that π'-accepts A.
3. Show that for any 5-cycle π, if there is a sequence of m instructions that π-accepts A then there is a sequence of m instructions that π-accepts the complement of A.

4. Show that if π and π' are 5-cycles, and there is a sequence of m instructions that π-accepts A, and a sequence of m' instructions that π'-accepts B, then there is a sequence of $2(m+m')$ instructions that π''-accepts $(A \cap B)$, for some 5-cycle π''. You may use the fact that there exist 5-cycles σ and τ whose commutator $\sigma\tau\sigma^{-1}\tau^{-1}$ is a 5-cycle. (You may wish to verify this fact for yourself).

5. Show that if π and π' are 5-cycles, and there is a sequence of m instructions that π-accepts A, and a sequence of m' instructions that π'-accepts B, then there is a sequence of $2(m+m')$ instructions that π''-accepts $(A \cup B)$, for some 5-cycle π''. Hint: write $A \cup B$ as an expression involving only complements and intersection, and use parts (c) and (d).

6. Show that if A is decided by a fan-in 2, depth d Boolean circuit with $\wedge, \vee$ and $\neg$ gates, then there is a sequence of at most 4^d instructions that π-accepts A, for some 5-cycle π. Hint: induction on d. Conclude that every language in non-uniform $\mathbf{NC}_1$ has a polynomial-size width-5 branching program.

7. Show that every language decided by polynomial-size width-5 branching programs is in non-uniform $\mathbf{NC}_1$. Conclude that the languages decided by polynomial-size width-5 branching programs are *exactly* non-uniform $\mathbf{NC}_1$.

Problem 2. The class $\mathbf{P/log}$ is the class of languages decidable by a Turing Machines running in polynomial time that take $O(\log n)$ bits of advice. Show that SAT$\in \mathbf{P/log}$ implies $\mathbf{P} = \mathbf{NP}$.